Australian National University
National Security College

Options for safeguarding undersea critical infrastructure

Australia and Indo-Pacific submarine cables

Samuel Bashfield and Anthony Bergin

Key Points

- Over 95 per cent of international communications and data transfers globally travel through submarine data cables.[1] These cables are "core critical infrastructure"[2], to the Internet, financial markets, and digital economies.
- As an island nation, Australia is particularly vulnerable* to submarine cable outages caused by different natural and man-made hazards. Indeed, many Indo-Pacific countries rely on a single line.
- Chinese firms are gaining market share in submarine cable services. While the industry has been dominated by American, European and Japanese interests, Chinese providers are increasingly contracted to lay, operate and maintain cable networks. China's involvement poses distinct data security risks for Indo-Pacific nations.
- The Australian government already helps to safeguard this critical technology and ensure connectivity and data integrity, but more can be done.

Key Recommendations

- Australia should continue to fund and co-fund submarine cable projects in the Indo-Pacific as alternatives to Chinese-backed proposals. It should also back the commitment made by the Northern Territory government to connect Australia to the trans-Pacific cable.
- To help promote Australia's submarine cable regime as the "gold standard", Australia should work with others to sponsor multilateral submarine cable vulnerability assessments and exercises to plan and develop protocols for timely responses to cable disruptions.
- At Indo-Pacfic multilateral meetings – such as the ASEAN Regional Forum, the Indian Ocean Rim Association, and the Pacific Islands Forum – Australia should support regional information and intelligence sharing concerning cable vulnerabilities and interference. These forums can be used to share information on vulnerable locations and promote ideas on best practice to integrate cable surveillance in national and regional maritime domain awareness systems.

As the critical infrastructure which enables global telecommunications, submarine cables form the backbone of how we communicate in the modern world. More than 400 submarine cables containing optical fibres cross the globe, covering some 1.3 million kilometres.[3] In the Indo-Pacific, submarine cables carry over 95 per cent of international data traffic, including telephone and data communications. But they are vulnerable to a variety of grave threats – including environmental (e.g. natural disasters), accidental (e.g. anchor damage) and malicious (e.g. cable sabotage) – which can generate acute economic consequences.

* 'Vulnerability', for the purposes of this paper, refers to nation-states at increased risk of submarine cable outages due to physical isolation (i.e. an island nation) or a lack of cable redundancy (i.e. connected to global networks by only one or two cables).

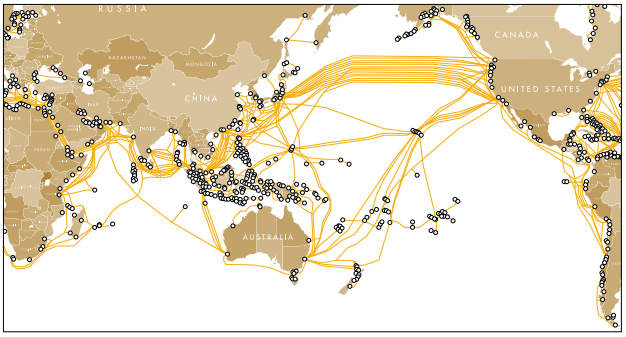

Figure 1: Indo-Pacific Submarine Cables[4]

Submarine cables underpin the global rise of cloud computing by providing low-latency and high capacity connections.[5] Cloud computing is an especially important element of modern information technology, allowing for distributed functions and relying on shared resources over the Internet.

Submarine cable security isn't just a matter for the states that cables connect: safeguarding cables is a shared responsibility. Cable disruptions can affect a myriad of users around the world simultaneously. Small island nations are particularly vulnerable if, as is the case in the Pacific, there is limited scope to branch off from multiple lines and they rely on a single cable.[6]

Submarine cables have failed due to natural hazards and negligence.[7] Anchor incidents caused parts of Egypt and India to be cut off in 2008 and disconnected Tonga for two weeks in 2019.[8] Tonga's submarine cable was severed again in January 2022 after a major volcanic eruption, which also triggered a tsunami.[9]

As China emerges as a major Indo-Pacific cable supplier, fears of cable-related espionage have grown. In 2021 the World Bank declined to award a contract to lay an undersea cable in the Pacific for regional fear China's HMN Tech would win.[10]

Submarine cables are laid, owned and maintained by the private sector. But governments have a responsibility to ensure the infrastructure conforms to security standards, and that there is sufficient redundancy to ensure resilience. It's not just the cables that are vulnerable, but also the landing points. Australia is connected via more than ten cables but with a handful of primary landing points in Perth and Sydney. It's surprising that the Australian government's civil maritime security strategy failed to note the importance of safeguarding our undersea cables and their importance for regional maritime security.[11]

Current challenges

Natural, commercial and recreational hazards

Of the 150 to 200 average cable faults that occur each year,[12] natural, commercial and recreational (e.g. boating) hazards are the principal cause. According to the International Cable Protection Committee, fishing and anchoring accounts for approximately 70 per cent of damage to submarine cables.[13] Damage can also be caused by earthquakes, landslides, volcanic activity and extreme weather. The persistence of these threats means that prompt access to submarine cable repair capabilities, operated by the private sector, is critical.

State and non-state risks

Acts of sabotage, interference and terrorism are persistent threats. Submarine cable locations (including landing sites) are publicly known, allowing interference by adversaries. Several Indo-Pacific states operate submarines that are capable of interfering with submarine cables.[14] It's very difficult to tap into a cable undetected, but much easier to do in data points or landing stations. These stations represent key vulnerabilities to data transmission security as data can be 'mirrored' once intercepted.[15]

Access to maintenance and repair services

In the event of submarine cable disruption, prompt access for repair crews is critical. Often these scarce repair vessels, operated by the private sector, are delayed not only by lengthy travel times to fault locations, but by bureaucratic barriers, including immigration, customs and excise procedures, security checks and approvals. These impediments, which need to be negotiated between the cable repairers and governments, often create long delays to cable repairs.[16]

Regulatory inadequacies

A regulatory gap exists in submarine cable protection. The United Nations Convention on the Law of the Sea (UNCLOS) is the primary (but not only) international legal regime for regulating submarine cables in international waters. However, many states don't fulfil obligations under UNCLOS, including criminalising conduct which has the potential to damage cables. Furthermore, existing international legal frameworks are inadequate to regulate the complex ownership structure of submarine cable infrastructure, which often does not clearly fall under the jurisdiction of any one country.[17] Further legal issues arise when submarine cables traverse contested and disputed maritime boundaries.

China as an emerging supplier

Globally, the four largest submarine cable contractors are SubCom (United States), NEC (Japan), Alcatel Submarine Networks (France, but now owned by Nokia), and HMN Tech (formerly Huawei Marine Networks).[18] HMN Tech, majority owned by Shanghai-based Hengtong Optic-Electric Co Ltd, has a global market share of approximately ten per cent, and has laid or repaired almost 100 of the world's 400 submarine cables. In 2021, the World Bank-sponsored East Micronesia Cable tender was cancelled due to fears HMN Tech would win. HMN Tech is listed in the US Department of Commerce 'Entity List,' which limits the supply of US material to the company.[19]

† Building a connecting branch to Darwin would be a vital enabler for the Australian Defence Force, national security more broadly and for digital access to Southeast Asia.

Recommendations to strengthen Indo-Pacfic submarine cable resilience

1. Fund Indo-Pacific submarine cables to avoid Chinese-backed alternatives

Australia should continue to monitor HMN Tech's proposals and tenders with Pacific states, and encourage and facilitate alternative suppliers where possible. Australia should continue funding cable projects in the Indo-Pacific, together with like-minded partners, such as Quadrilateral Security Dialogue members,[20] France, the UK and the EU's Global Gateway program to connect vulnerable nations and avoid Chinese-backed alternatives.

Australia should also back the commitment made by the Northern Territory government to connect Australia to the trans-Pacific cable, which will enhance digital connectivity between Australia and the United States and support critical infrastructure in the Indo-Pacific.[21] This will be the only subsea cable that connects the US to Singapore with a national security rated capability which doesn't transit the South China Sea. It's a secure, low-latency, high speed data link to the US and Asia.†

2. Promote the Australian submarine cable protection regime as a regional "gold standard"

Australian legislation should serve as a template for both Indian Ocean and Pacific Island states, when legislating for the protection of submarine cables in their respective national jurisdictions. Australia's *Telecommunications Act 1997* allows the Australian government to declare a "protection zone" around submarine cables within Australian territory, restricts certain potentially damaging activities within protection zones, sets out stringent criminal offenses for unlawful conduct and stipulates that telecommunication carriers must apply for government permits to install cables.[22] Figure 2 illustrates the Northern Protection Zone located in Sydney's northern beaches. Similar zones are enforced off Sydney's eastern beaches area and off Perth's coast.

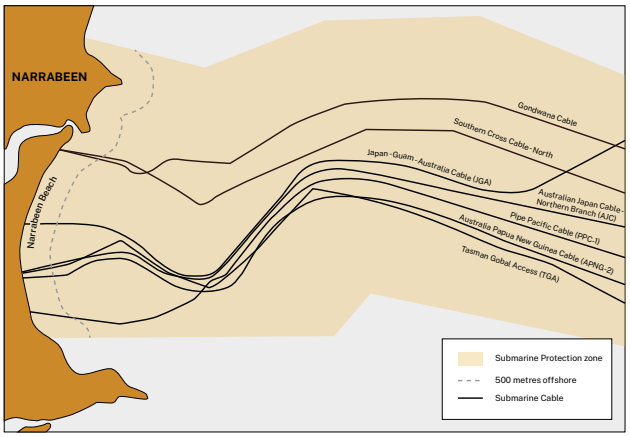

Figure 2: Northern Submarine Cable Protection Zone, Sydney, Australia.[23]

These provisions effectively mitigate the threats to submarine cables from commercial and recreational activity in Australia's territorial waters. The regime is considered world-leading.

Key legislative measures which could be exported include publishing submarine cable zone maps for maritime users, banning certain types of activities within protection zones, creating criminal offenses for those endangering cables and effective surveillance and law enforcement.

Promoting the adoption of similar legislation throughout the Indo-Pacific will assist more nations to comply with UNCLOS obligations and better safeguard cables from accidental damage and breaks.

3. Undertake multilateral submarine cable vulnerability assessments and exercises

Australia, along with allies and partners, should sponsor multilateral exercises on attack scenarios that imply large scale cable breaks on several cables and repair infrastructure. This initiative would bring toegther government officials and industry representatives to plan and develop protocols for quick repairs and responses to cable disruptions.

A focus should be on scenarios where many cables are severed in a short time period, assessing the available redundancies and any legislative and capability gaps that might exist across the region. Such exercises should assist in reducing bureaucratic barriers which hamper the prompt attendance by cable repair ships, including immigration, customs and excise procedures, security checks and approvals/permissions.

4. Encourage greater information sharing and regional maritime domain awareness

Using Indo-Pacfic multilateral fora, such as the ASEAN Regional Forum, the Indian Ocean Rim Association and Pacific Islands Forum, Australia should encourage information sharing concerning cable vulnerabilities and interference. These forums should promote best practice on integrating cable surveillance into national and regional maritime domain awareness systems and establish regional registers for government and industry points of emergency contact on cable resilience.

Endnotes

1. Lionel Carter and Douglas R. Burnett, 'Subsea Telecommunications', in *Routledge Handbook of Ocean Resources and Management,* ed. Hance D. Smith, Juan Luis Suarez de Vivero, and Tundi S. Agardy, Routledge Environment and Sustainability Handbook (Abingdon: Routledge, 2015).
2. Christian Bueger and Tobias Liebetrau, 'Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network', *Contemporary Security Policy* 42, no. 3 (3 July 2021): 391, https://doi.org/10.1080/13523260.2021.1907129.
3. Pierre Morcos and Colin Wall, 'Invisible and Vital: Undersea Cables and Transatlantic Security', Center for Strategic and International Studies, 11 June 2021, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security.
4. Indo-Pacific Submarine Cable Map (TeleGeography, 8 July 2021), https://www.submarinecablemap.com/#/.
5. Jonathan E. Hillman, 'Securing the Subsea Network: A Primer for Policymakers', Reconnecting Asia Project (Washington DC: Center for Strategic and International Studies, March 2021), 3, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210309_Hillman_Subsea_Network_1.pdf?1c7RFgLM3w3apMi0eAPl2rPmqrNNzvwJ.
6. Amanda H.A. Watson, 'Undersea Internet Cables in the Pacific: Part 2: Cybersecurity, Geopolitics and Reliability', ANU Department of Pacific Affairs, In Brief 2021/20, 2021, http://dpa.bellschool.anu.edu.au/sites/default/files/publications/attachments/2021-08/undersea_internet_cables_in_the_pacific_part_2_-cybersecurity_geopolitics_and_reliability_amanda_h_a_watson_department_of_pacific_afffairs_in_brief_2021_20.pdf.
7. Robert Beckman, 'Protecting Submarine Cables from Intentional Damage: The Security Gap', in *Submarine Cables: The Handbook of Law and Policy, ed. D.R Burnett, R. Beckman, and T.M. Davenport (Leiden: Brill, 2013), 282.*
8. Tom Westbrook, 'Severed Cable Sends Tonga "Back to Beginning of the Internet"', Reuters, 24 January 2019, https://www.reuters.com/article/us-tonga-internet-idUSKCN1PI0A8.
9. Tom Pullar-Strecker, 'Tonga Subsea Communications Cable "May Be Broken after All", Says Southern Cross', News, Stuff, 16 January 2022 https://www.stuff.co.nz/business/127512800/tonga-subsea-communications-cable-may-be-broken-after-all-says-southern-cross. It took longer than a month for the cable to be repaired.
10. Jonathan Barrett and Yew Lun Tian, 'Pacific Undersea Cable Project Sinks after U.S. Warns against Chinese Bid', *Reuters*, 18 June 2021, https://www.reuters.com/world/asia-pacific/exclusive-pacific-undersea-cable-project-sinks-after-us-warns-against-chinese-2021-06-18/.
11. 'Australian Government Civil Maritime Security Strategy' (Canberra: Australian Department of Home Affairs, 2022), https://www.homeaffairs.gov.au/nat-security/files/australian-government-civil-maritime-security-strategy.pdf.
12. Carter and Burnett, 'Subsea Telecommunications', 353.
13. 'Government Best Practices for Protecting and Promoting Resilience of Submarine Telecommunications Cables' (Lymington, United Kingdom: International Cable Protection Committee, 13 July 2021), https://www.iscpc.org/publications/icpc-best-practices/.
14. Thomas Newdick, 'Norwegian Undersea Surveillance Network Had Its Cables Mysteriously Cut', The Drive, 11 November 2021, https://www.thedrive.com/the-war-zone/43094/norwegian-undersea-surveillance-network-had-its-cables-mysteriously-cut.
15. Olga Khazan, 'The Creepy, Long-Standing Practice of Undersea Cable Tapping', The Atlantic, 16 July 2013, https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.
16. 'Economic Impact of Submarine Cable Disruptions', Research (Bangkok: Asia-Pacific Economic Cooperation Policy Support Unit, 2013), 68, https://www.apec.org/docs/default-source/Publications/2013/2/Economic-Impact-of-Submarine-Cable-Disruptions/2013_psu_-Submarine-Cables.pdf.
17. Douglas R. Burnett, 'Submarine Cable Security and International Law', *International Law Studies* 97 (2021): 1668, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2992&context=ils.
18. Huawei sold HMN following the US blacklisting of Huawei in 2019; *Quad Economy & Technology Task Force Report: A Time for Concerted Action,* Gateway House, August 2021, https://www.gatewayhouse.in/wp-content/uploads/2021/08/Quad-Economy-and-Technology-Task-Force-Report_GH_2021.pdf.
19. 'Quad Tech Network', National Security College (The Australian National University), 5, accessed 12 March 2021, https://nsc.crawford.anu.edu.au/department-news/18328/quad-tech-network.
20. GatewayHouse, 'A Time for Concerted Action among Quad Countries: Gateway House Task Force Report', *Gateway House* (blog), 30 August 2021, https://www.gatewayhouse.in/gateway-house-task-force-report/; Hayley Channer, 'Promise Less, Deliver More: Quad's Best Answer to China', *Sydney Morning Herald,* 10 February 2022, https://www.smh.com.au/national/promise-less-deliver-more-quad-s-best-answer-to-china-20220209-p59v30.html.
21. 'Joint Statement Australia-U.S. Ministerial Consultations (AUSMIN) 2021', Australian Government Department of Foreign Affairs and Trade, 2021, https://www.dfat.gov.au/geo/united-states-of-america/ausmin/joint-statement-australia-us-ministerial-consultations-ausmin-2021.
22. 'Telecommunications Act 1997', C2021C00237 § 3A (2021), https://www.legislation.gov.au/Details/C2021C00237.
23. 'Northern Protection Zone - Inshore Detail', Australian Communications and Media Authority, 31 August 2021, https://www.acma.gov.au/sites/default/files/2021-09/NPZ_2021.pdf.

About the Authors

Samuel Bashfield is a PhD candidate, research officer and tutor at the ANU National Security College. Sam's research engages with Indian Ocean security issues, with a focus on the past, present and future of the Chagos Archipelago (British Indian Ocean Territory).

Anthony Bergin is a Senior Fellow with the Australian Strategic Policy Institute and researches and writes on a wide range of Indo-Pacific maritime security issues.

About the Editor

Dr William A. Stoltz is the Manager of Public Policy at the ANU National Security College. He is responsible for mobilising the College's research and resident expertise to influence and inform current public policy debates.